



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/431,067	11/01/1999	AMIR HERZBERG	HERZBERG=1	8218

1444 7590 09/30/2003

BROWDY AND NEIMARK, P.L.L.C.
624 NINTH STREET, NW
SUITE 300
WASHINGTON, DC 20001-5303

EXAMINER

SMITHERS, MATTHEW

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 09/30/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/431,067

Applicant(s)

HERZBERG ET AL.

Examiner

Matthew B Smithers

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 01 November 1999.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-25 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-6, 11-18 and 23-25 is/are rejected.
- 7) ☒ Claim(s) 7-10 and 19-22 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 4.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other:

DETAILED ACTION

Information Disclosure Statement

The information disclosure statement filed October 11, 2000 has been placed in the application file and the information referred to therein has been considered as to the merits.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 11, 12, 23 and 24 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2134

Claims 1-6, 11-18, 24 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. patent 6,035,041 granted to Frankel et al as and further in view of U.S. patent 6,185,678 granted to Arbaugh et al.

Regarding claims 1, 13, and 25, Frankel teaches a proactive public key system where each server has a private key share of a common public key between the group of servers. The proactive system initiates a procedure for restoring the group of proactive server using the key shares (see Abstract and column 10, line 62 to column 12, line 18). Frankel fails to specifically teach the restoring procedure using the individual server's public key information. Arbaugh teaches a network environment where public key information from a computing system's ROM is used to restore the computing system (see Abstract and column 10, lines 47-67). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Arbaugh's system for secure automated recovery of active network elements with Frankel's proactive network system in order to gain the advantage of ensuring the integrity of the information used in the recovery procedure of the computing system [see Arbaugh; column 4, lines 38-45].

Regarding claims 2 and 14, Frankel et al and Arbaugh et al disclose everything claimed as applied above (see claims 1 and 13, respectively), in addition, Frankel teaches restore procedure is invoked by refresh procedure (see column 11, lines 9-10 and column 12, lines 9-14).

Regarding claims 3 and 15, Frankel et al and Arbaugh et al disclose everything claimed as applied above (see claims 1 and 13, respectively), in addition, Arbaugh

Art Unit: 2134

teaches non erasable part of the storage being a ROM memory module (see column 10, lines 47-67).

Regarding claims 4 and 16, Frankel et al and Arbaugh et al disclose everything claimed as applied above (see claims 1 and 13, respectively), in addition, Arbaugh teaches wherein said applications being, at least one of the following: Secure logging, Secure end-to-end communication, Timestamping, Certificate authority, Key recovery, Voting, Trading, Database, Operating system, Access control mechanisms, Secure Commerce (see column 17, line 32 to column 18, line 30).

Regarding claims 5 and 17, Frankel et al and Arbaugh et al disclose everything claimed as applied above (see claims 1 and 13, respectively), in addition, Arbaugh teaches restore related information includes restore related self information (see column 10, lines 47-67).

Regarding claims 6 and 18, Frankel et al and Arbaugh et al disclose everything claimed as applied above (see claims 1 and 13, respectively), in addition, Frankel teaches restore related information includes restore related others' information (see column 10, line 62 to column 12, line 18).

Regarding Claims 11 and 23, Frankel et al and Arbaugh et al disclose everything claimed as applied above (see claims 1 and 13, respectively), in addition, Arbaugh teaches an initialize procedure (see column 6, lines 7-24).

Regarding Claims 12 and 24, Frankel et al and Arbaugh et al disclose everything claimed as applied above (see claims 1 and 13, respectively), in addition, Frankel teaches a restore procedure (see column 10, line 62 to column 12, line 18).

Allowable Subject Matter

Claims 7-10, and 19-22 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter:

With respect to claims 7 and 19, the cited prior art fails to specifically teach wherein said restore related self information includes $M_I = S_{start}^I (V_{Cert}, C)$.

With respect to claims 8 and 20, the cited prior art fails to specifically teach wherein said restore related others' information includes $(S_{Cert}(M), M)$.

With respect to claims 9 and 21, the cited prior art fails to specifically teach wherein said initialization procedure includes:

- (i) input for receiving at least configuration data C , public non-proactive related key V_{start}^I and discardable one time private key S_{start}^I ;
- (ii) the processor generating a set of keys $S_I(0)$, $V_I(0)$, $E_I(0)$, $D_I(0)$;
- (iii) broadcasting said set of keys except $D_I(0)$ over the network to the rest of the servers $(1, \dots, i-1, i+1, \dots, n)$ in the group, so as to authenticate and encrypt the network channel;
- iv) the processor generating the group public proactive key V_{Cert} and a share (S_{CERT}^I) of corresponding private proactive key S_{CERT} ;

Art Unit: 2134

(v) the processor generating restore related self information that includes $M_i = S_{start}^I, (V_{cert}, C)$.

(vi) discarding the one-time private key S_{start}^I ;

(vii) broadcasting M_i to all servers in the group, and receiving M_j from all respective SP_j servers in the group; the processor concatenating said $M_1 \dots M_N$ so as to construct M ;

(viii) the processor generating a joint signature $(S_{cert}(M), M)$ that forms part of said restore related others' information; and

(ix) broadcasting the joint signature $(S_{cert}(M), M)$.

With respect to claims 10 and 22, the cited prior art fails to specifically teach wherein said recover procedure includes:

(i) the processor extracting V_{start}^I ;

(ii) the processor extracting M^I from M ; the processor constructing V_{cert} by applying V_{start}^I to M^I ;

(iv) the processor validating M by applying V_{cert} to the joint signature part $(S_{cert}(M))$; if the result matches M then the server becomes operational; sending M and $S_{cert}(M)$ to all the group servers;

(v) if, on the other hand, M is invalid, then waiting the receipt of another joint signature and in response repeating said (ii) to (iv).

Conclusion

Art Unit: 2134

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.


A. Frankel et al (6,237,097) discloses a robust efficient distributed system.

B. Jakobsson (6,587,946) discloses a system for a quorum controlled public key encryption.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B Smithers whose telephone number is (703) 308-9293. The examiner can normally be reached on Monday-Friday (9:00-5:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.


Matthew B Smithers
Primary Examiner
Art Unit 2134